УДК 681.3.06: 519.248.681

В. И. ДОЛГОВ, д-р техн. наук, И. В. ЛИСИЦКАЯ, канд. техн. наук, В. И. РУЖЕНЦЕВ

ОБЕСПЕЧЕНИЕ СТОЙКОСТИ ШИФРА DES К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА. ПЕРЕКРЫТИЕ ИТЕРАТИВНЫХ ХАРАКТЕРИСТИК ОБНУЛЯЮЩЕГО ТИПА И ЧЕТЫРЕХЦИКЛОВЫХ ИТЕРАТИВНЫХ ХАРАКТЕРИСТИК

Идея построения *S*-блоков для шифра DES, обеспечивающих его устойчивость к атакам линейного и дифференциального криптоанализов (ЛК и ДК), сегодня уже не нова [1,2,5,6,10]. В этой работе мы хотим представить новую версию решения этой задачи применительно к ДК. Стимулом к появлению и формированию излагаемого подхода стали некоторая незавершенность известных результатов в этом направлении и новые соображения, появившиеся в процессе изучения принципов защиты шифра DES от атак ЛК, изложенные в работе [11].

Напомним, что основой реализации атак линейного и дифференциального криптоанализов является использование линейных либо дифференциальных характеристик (ЛХ и ДХ), описывающих прохождение через циклы шифрования специфических открытых текстов (плайнтекстов) или пар плайнтекстов, с помощью которых можно ставить и решать задачи криптоанализа со сложностью меньшей, чем прямой перебор ключей (атаки грубой силы). В работе [11] рассмотрены принципы построения ЛХ шифра DES, основанные на изучении графов переходов. Здесь мы хотим развить эту же идею применительно к построению и оценке вероятностей ДХ. Все дело в том, что между ДХ и ЛХ шифра DES существует простая и однозначная связь, которая заключается в том, что дифференциальные характеристики могут рассматриваться как обратное (с точки зрения направления переходов) отображение линейных аппроксимационных характеристик. В работе [12] эта особенность отмечена указанием на то, что в дифференциальных характеристиках свободной является левая часть, в то время как в линейных – правая. Имеется также еще одно существенное отличие в образовании линейных и дифференциальных характеристик. Оно заключается в том, что в построении дифференциальных характеристик участвуют не маски, а реальные значения входов и выходов *S*-блоков. Поэтому, если в линейных характеристиках маски входов отдельных *S*-блоков могут принимать произвольные значения (в том числе содержать входные биты *S*-блоков, не задействованных в переходе, и поэтому нельзя по входной маске определить активизируемые *S*-блоки), то в дифференциальных характеристиках композиции входных битов однозначно определяют *S*-блоки, участвующие в характеристике. Итеративные дифференциальные характеристики для шифра DES, построенные в соответствии с отмеченной идеей, для числа циклов не превышающего 10, изображены на рис. 1.

Отметим еще раз, что общей методологической основой формирования (исследования) условий повышения сопротивляемости шифра DES к атакам ДК и ЛК, является выполнение требований к *S*-блокам, сформулированных разработчиками стандарта [5,14]. В работе [2] было уже показано, что большинство из этих требований (6 из 8-ми) направлено именно на защиту от атак ДК. Здесь мы напомним эти требования в редакции работы [14]:

1. Каждый *S*-блок имеет 6 входных и 4 выходных бита;

2. Нет выходного бита *S*-блока, который может быть связан функцией близкой к линейной с входными битами;

3. Если зафиксированы самый левый и самый правый входные биты *S*-блока и изменяются четыре его средних бита, то каждый из возможных 4-битовых выходов получается точно один раз ($S(\mathbf{x}) \neq S(\mathbf{x} \oplus 0abcd0)$ для любых a, b, c и d, $abcd \neq 0000$);

1. Если два входа *S*-блока отличаются точно одним битом, то выходы должны отличаться не менее чем в двух битах;

4. Если два входа *S*-блока отличаются точно в двух средних битах, то выходные биты должны отличаться не менее чем двумя битами ($S(\mathbf{x}) \neq S(\mathbf{x} \oplus 001100)$);

5. Если два входа *S*-блока отличаются своими первыми двумя битами и имеют совпадающими два последних бита, то выходные биты не должны быть теми же самыми ($S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef00)$ для любых e и f);

6. Для любых ненулевых 6-битовых различий между входами не более чем 8 из 32 пар входов могут показывать одни и те же выходные различия;

8. Критерий, подобный седьмому, должен выполняться и в случае трех активных *S*-блоков.

1

$0_x \leftarrow \Gamma$

$0_x \leftarrow 0_x$

2-х цикловая итеративная характеристика

2

$\Phi \leftarrow \Gamma$

$0_x \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

4-х цикловая итеративная характеристика

3

$\Phi \leftarrow \Gamma$

$\Gamma \oplus \Psi \leftarrow \Theta$

$\Phi \leftarrow \Psi$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

4-х цикловая итеративная характеристика

4

$\Phi \leftarrow \Gamma$

$\Gamma \leftarrow \Phi$

$0_x \leftarrow 0_x$

$\Gamma \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

6-ти цикловая итеративная характеристика

5

$\Phi \leftarrow \Gamma$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Psi$

$\Gamma \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Theta$

6-ти цикловая итеративная характеристика

6

$\Phi \leftarrow \Gamma$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Psi$

$\Gamma \oplus \Psi \leftarrow \Phi$

$\Theta \leftarrow \Gamma$

$\Psi \leftarrow \Phi \oplus \Theta$

$\Phi \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Theta$

8-ми цикловая итеративная характеристика

7

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi$

$\Phi \leftarrow \Gamma \oplus \Psi$

$0_x \leftarrow 0_x$

$\Phi \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

8-ми цикловая итеративная характеристика

8

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi$

$\Theta \leftarrow \Gamma \oplus \Psi$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$0_x \leftarrow 0_x$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

10-ти цикловая итеративная характеристика

9

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Gamma \oplus \Psi$

$\Gamma \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow \Psi$

$\Gamma \oplus \Psi \leftarrow \Theta$

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi \oplus \Theta$

$\Phi \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Theta$

10-ти цикловая итеративная характеристика

Рис. 1

В работе [2] сделан вывод, что на время появления стандарта его действительно можно было считать неуязвимым к атакам ДК. Однако, разработанный позднее Эли Бихамом и Ади Шамиром метод ДК [12,13] позволил осуществить атаку на 16-цикловый DES со сложностью меньшей прямого перебора всех ключей (атаки "грубой силой"). Ограничений к отбору *S*-блоков, предложенных разработчиками стандарта, уже оказалось недостаточно для защиты от этой атаки. Об этом свидетельствуют и расчеты, приведенные в работе [2]. Последующие исследования, как уже было отмечено выше, позволили определить дополнительные ограничения к отбору *S*-блоков, позволяющие повысить сопротивляемость шифра DES атакам ДК.

Задачей настоящей работы и является более строгое обоснование необходимых дополнительных ограничений.

1. Обеспечение сопротивляемости атакам ДК с использованием итеративных характеристик обнуляющего типа

Самыми опасными для атак ДК, как следует из результатов анализа и расчетов [2], являются итеративные дифференциальные характеристики обнуляющего типа. Так в [2] названы характеристики, строящиеся с помощью "обнуляющего" разностного преобразования, при котором ненулевая разность на входе цикловой функции F преобразуется в нулевую разность на ее выходе. Этому случаю соответствуют характеристики под номерами 1 и 2, представленные на рис. 1. В работе [2] показано, что атаки ДК на одноблочные и двухблочные характеристики этого типа разработчики стандарта перекрыли с помощью выполнения при отборе *S*-блоков требований 3 и 6 (см. критерии отбора *S*-

блоков стандарта, представленные выше). Однако для перекрытия атаки Бихама на характеристики обнуляющего типа с числом S-блоков большем 2, ограничений использованных разработчиками уже оказывается недостаточно. В атаке используется 13-цикловая ДХ на циклах со 2-го по 14-й с последующей 2R-атакой на 15-м и 16-м циклах. При этом первый цикл подбирается специальным образом. Сама 13-цикловая характеристика строится, как уже отмечалось выше, путем итеративного повторения шести с половиной раз трехблочной двухцикловой итеративной ДХ обнуляющего типа. Эли Бихам и Ади Шамир обнаружили две трехблочные итеративные ДХ обнуляющего типа, имеющие вероятность $p_T = \frac{1}{234}$, что привело к вероятности всей 13-цикловой характеристики, равной

$$(p_T)^{\frac{n-4}{2}} = p_T^6 = 2^{-47.2}.$$

Этот результат позволил Эли Бихаму, имея $\approx 2^{48}$ отобранных открытых текстов, предложить процедуру определения ключей шифрования, которая оказалась менее сложной, чем их прямой перебор. И здесь мы подходим к обоснованию первого из дополнительных критериев отбора S-блоков для шифра DES, которое мы сформулируем в виде Условия 1.

Условие 1 (У-1). Для защиты от атак ДК на основе использования итеративных двухцикловых ДХ обнуляющего типа с числом активных S-блоков в двух циклах, меньшем восьми, необходимо и достаточно, чтобы дополнительно к требованию 6 разработчиков стандарта S-блоки не имели переходов в ноль еще для четырех входов: 32_x, 36_x, $3A_x$, $3E_x$ ($S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef10)$).

Отметим, что к этому же ограничению пришли (по времени, как оказалось, раньше нас) и корейские ученые [5].

Справедливость утверждения У-1 легко устанавливается из анализа табл. 3 нашей работы [2], в которой показано участие S-блоков в формировании входной разности для трехблочной характеристики.

Заметим также, что уже для пятиблочной итеративной ДХ обнуляющего типа в самом благоприятном для криптоаналитика случае, когда обнуляющие переходы через все активные S-блоки имеют максимальную вероятность $\frac{16}{64}$ (в соответствии с требованием 7 разработчиков стандарта), получаем граничное значение вероятности для всей 13-цикловой ДХ

$$\left[\left(\frac{16}{64}\right)^5\right]^6 = 2^{-60}.$$

Таким образом, выполнение требований разработчиков стандарта 3, 6 и 7 и дополнительного ограничения У-1 позволяет сделать характеристики 1 и 2 (рис. 1) нереализуемыми.

2. Обеспечение сопротивляемости атакам ДК, использующим четырехцикловые итеративные ДХ без тождественных циклов

Рассмотрим теперь возможности проведения атаки с использованием ДХ, составленных из четырехцикловых итеративных характеристик, представленных под номером 3 на рис. 1.

Здесь нас должны интересовать ДХ с общим числом активных S-блоков, приходящихся на итеративную характеристику, не превышающим восьми, так как для 13 циклов результирующие вероятности для ДХ, составленных из четырехцикловых ДХ с восемью и девятью S-блоками, будут ограничены следующими значениями:

$$\left[\left(\frac{16}{64}\right)^8\right]^3 \cdot \left(\frac{16}{64}\right)^2 = 2^{-50}, \left[\left(\frac{16}{64}\right)^9\right]^3 \cdot \left(\frac{16}{64}\right)^2 = 2^{-58}.$$

Рассмотрим сначала ДХ минимального типа. Таковыми мы будем называть ДХ, которые строятся с использованием минимального числа битов входов и выходов для задействованных S-блоков. В этом случае каждому символу характеристики 3 (рис. 1) можно поставить в соответствие один бит (входа или выхода) S-блока. Сразу отметим, что в рамках принятых обозначений входов и выходов задействованных S-блоков наряду с характеристикой 3 (рис. 1) можно рассматривать еще несколько

вариантов четырехцикловых ДХ, которые вместе с исходной представлены на рис. 2. Рассмотрим отдельно каждую из этих характеристик.

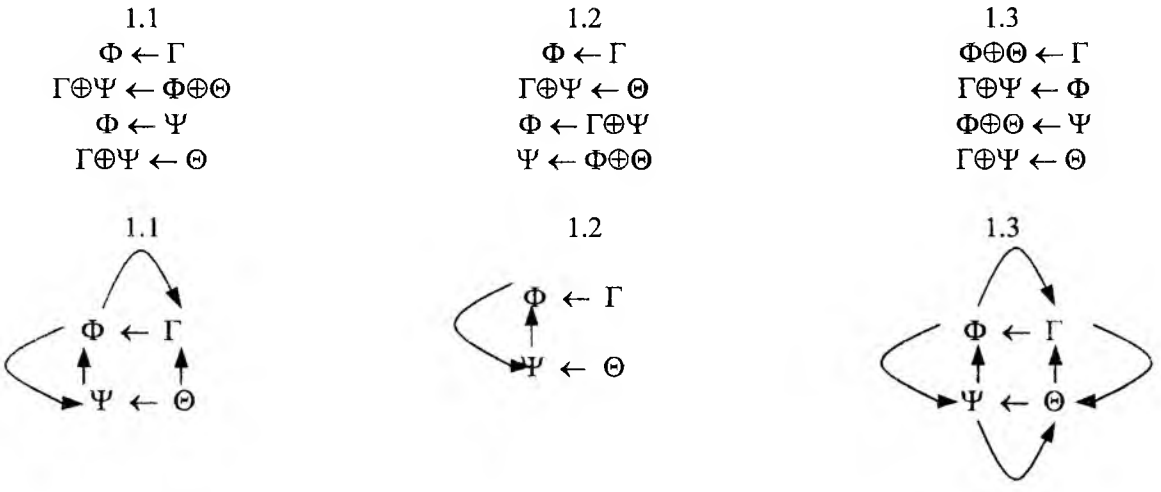

Рис. 2

Для ДХ минимального типа 1.1 (рис. 2) входы Г, Ψ и Θ – однобитные. Из допустимости перехода Г⊕Ψ←Θ, очевидно, следует считать допустимыми и переходы Г←Θ и Ψ←Θ. В результате мы приходим к графу переходов для рассматриваемой характеристики, представленному под соответствующим номером на рис. 2. Подчеркнем здесь, однако, что для рассматриваемой ДХ это совсем не означает, что должен быть допустимым и переход Г⊕Ψ←Ф.

Аналогичные рассуждения приводят к графам переходов других вариантов характеристик минимального типа, также изображенным под соответствующими номерами на рис. 2. Примеры построения характеристик с графами переходов 1.1, 1.2 изображены на рис. 3.

1.1

17 ← 3 (2),(30,31,32) 1 (2)
1,3 ← 16,17 (14,15,18,19) 2
17 ← 1 (2),(30,31,32) 2
1,3 ← 16 (14,15,18,19) 2

Здесь входы 1_x (C_x или E_x), и еще (E_x) переходят в ноль

1.2

17 ← 2 1
3 ← 18 (14,15,16,19) 1 (2)
17 ← 2,3 1
3 ← 17,18 (14,15,16,19) 2

Здесь вход 1_x переходит в ноль или входы (E_x) и (F_x).

1.1

15 ← 30, (31) 1
28,30 ← 8,15, (6,7,9,10,11) 3
15 ← 28 (31) 2
28,30 ← 8 (6,7,9,10,11) 2

Здесь входы 1_x и 4_x переходят в ноль

1.2

17 (18) ← 3 (2) 1
4 ← 21 (18,19,20,22,23) 2
17 (18) ← 3,4 (2) 2
4 ← 17,21 (18,19,20,22,23) 3

Здесь входы 1_x (F_x), 11_x($1F_x$), 20_x переходят в ноль

Рис. 3

Все характеристики на этом рисунке представлены как в минимальном изображении, так и в случае использования дополнительных битов входов (в скобках).

На рис. 4 приведены примеры четырехцикловых характеристик неминимального типа, которые содержат дополнительные биты не только входов, но и выходов задействованных *S*-блоков.

Покажем, что в построении всех приведенных на рис. 3 ДХ минимального типа принимают участие *S*-блоки с однобитными переходами и (или) нулевыми выходами

Рассмотрим сначала характеристику 1.1 (рис. 2). Очевидно, что для двух одинаковых однобитных выходов Ф такой характеристики минимального типа соответствующие им однобитные входы Г и Ψ должны быть различными входами в одни и те же (идентичные) *S*-блоки, которые своими совпадающими (однобитными) выходами Ф инициируют вход промежуточного цикла, формирующего в свою очередь различные однобитные ненулевые входы Г и Ψ соответствующих циклов. Учитывая *P*-

перестановку, используемую в стандарте, в один и тот же *S*-блок можно попасть различными битовыми входами только из двух *S*-блоков. Следовательно, переходы Г⊕Ψ←Θ и Г⊕Ψ←Ф⊕Θ – как минимум двухблочные, и тогда однобитный вход Θ непременно должен быть общим входом двух смежных (соседних) *S*-блоков.

1.1		1.1	
(17) 18 ← 3 (5),(2,6,7)	2	(15) 17 ← 3 (2),32	1 (2)
3,4 ← 21 (23),(19,20,22)	2	1,3 ← (15) 16,17 (14,18,19)	2
(17) 18 ← 4 (5),(2,6,7)	2	(15) 17 ← 1 (2),32	2
3,4 ← (17) 18,21 (23),(19,20,22)	3	1,3 ← 16 (14,18,19)	2

Рис. 4

Убедимся теперь в том, что и один из двух циклов с совпадающими выходами Ф также будет двухблочным. Действительно, для одноблочных циклов необходимо, чтобы их входы Г и Ψ были внутренними битами (одним из двух) шестибитных входов *S*-блоков этих циклов. На рис. 5 представлены все возможные варианты однобитных входов в *S*-блоки, активизирующие двухбитные входы одного и того же *S*-блока следующего цикла (переход Г⊕Ψ←Θ).

Как следует из приведенных данных, во всех случаях один или оба бита для всех возможных вариантов двухбитных выходов (входов) не удовлетворяют указанному выше условию. Поэтому, как минимум один из двух циклов с переходом в Ф является двухблочным. В результате, если рассматриваются ДХ минимального типа, то общее число активных *S*-блоков, приходящихся на четырехцикловую ДХ, может быть самое меньшее равным семи, причем, один из двухблочных циклов (Г⊕Ψ←Θ или Г⊕Ψ←Θ⊕Ф) строится с использованием двух однобитных переходов, а второй (Ф←Г или Ф←Ψ) – наряду с однобитным переходом содержит и переход в ноль (один из выходов двух *S*-блоков цикла с единственным битом выхода будет нулевым).

$$4 \text{ или } 5 \Rightarrow \begin{cases} 17,18 \\ 28,31 \\ 13,17 \end{cases} \qquad 8 \text{ или } 9 \Rightarrow \begin{cases} 16,18 \\ 28,30; \\ 13,16 \end{cases} \qquad 12 \text{ или } 13 \Rightarrow \begin{cases} 24,26 \\ 16,20; \\ 20,24 \end{cases}$$

$$16 \text{ или } 17 \Rightarrow \begin{cases} 25,26 \\ 1,3 \quad ; \\ 20,25 \end{cases} \qquad 20 \text{ или } 21 \Rightarrow \begin{cases} 4,8 \\ 25,29; \\ 3,4 \end{cases} \qquad 24 \text{ или } 25 \Rightarrow \begin{cases} 29,32 \\ 11,12 ; \\ 4,7 \end{cases}$$

$$28 \text{ или } 29 \Rightarrow \begin{cases} 21,22 \\ 12,15; \\ 5,7 \end{cases} \qquad 32 \text{ или } 1 \Rightarrow \begin{cases} 5,9 \\ 15,17. \\ 21,23 \end{cases}$$

Рис. 5

Следовательно, общей особенностью характеристик 1.1 минимального типа является использование при их построении *S*-блоков с однобитными переходами и переходов одного бита входа в ноль (как показывает анализ, переходы в ноль будут характерными во многих случаях и для другой пары циклов четырехцикловой характеристики). Но в соответствии с требованиями 3 и 4 разработчиков стандарта переходы одного бита входа в один бит выхода и одного бита входа в ноль для *S*-блоков запрещены. Поэтому четырехцикловые характеристики типа 1.1 минимального типа для шифра DES нереализуемы.

Если рассматривать характеристики типа 1.1 неминимального типа, то из приведенных примеров (рис. 3, рис. 4) видно, что для большинства из них также оказывается характерным использование переходов в ноль, для которых соответствующие ограничения разработчиков стандарта делают их нереализуемыми (вероятности этих характеристик оказываются равными нулю). В то же время все же имеется возможность (за счет свободы в выборе входов и выходов *S*-блоков) построить четырехцикловые характеристики, использующие переходы в ноль, не попадающие под ограничения разработчиков стандарта. При этом можно получить и характеристики, не использующие однобитные переходы. Для характеристик 1.1 мы в лучшем случае приходим как минимум к восьмиблочным характери-

стикам, все циклы которых содержат пары S-блоков. Примеры построения таких характеристик представлены на рис. 6.

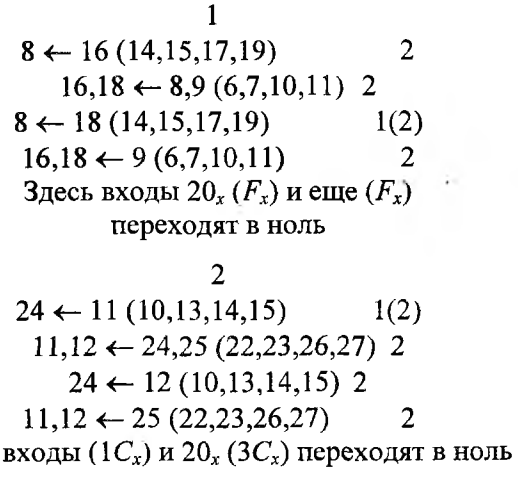

Рис. 6

Как следует из приведенных примеров, характеристики минимального типа и здесь нереализуемы. В то же время, при использовании дополнительных битов входов действительно можно получить S-блоки с нулевыми выходами (входы F_x для характеристики 1 (рис. 6) и входы $1C_x$ и $2C_x$ для характеристики 2 (рис. 6)) для входов, куда попадают биты инициирующие разные строки таблицы подстановок S-блоков. Соответственно, дополнительные биты входов позволяют уйти и от однобитных переходов.

Чтобы определить дополнительные ограничения для таких характеристик заметим, что общей особенностью всех четырехцикловых характеристик является то, что они содержат пары S-блоков, для которых побитовая сумма по модулю 2 входов равна 1 или 2, т.е. $W(\alpha_1 \oplus \alpha_2) = 1$ или $W(\alpha_1 \oplus \alpha_2) = 2$, в то время как соответствующие выходы S-блоков совпадают: $\beta_1 = \beta_2 = \beta$. Поэтому для перекрытия четырехцикловых характеристик, не попадающих под ограничения разработчиков стандарта, предлагается ввести следующее, на наш взгляд, достаточно мягкое условие.

Условие 2 (У-2) (условие перекрытия четырехцикловых итеративных характеристик). Элементы таблицы дифференциальной разности каждого S-блока, для которых $W(\alpha_1 \oplus \alpha_2) = 1$ или $W(\alpha_1 \oplus \alpha_2) = 2$, при этом $\beta_1 = \beta_2 = \beta$, должны подчинятся следующему ограничению:

$$NS_k(\alpha_1,\beta) \cdot NS_k(\alpha_2,\beta) \le 160,$$

где $W(a)$ – вес по Хэммингу числа a; β – выходная 4-битная разность; α_1, α_2 – входные 6-битные разности; $NS_k(a,b)$ – число случаев, когда разность a на входе k-го S-блока переходит в выходную разность b.

Этому условию удовлетворяют не менее двух пар S-блоков для любой характеристики 1.1 неминимального типа, содержащей не менее 8 активных S-блоков (в которой отсутствуют нулевые выходы S-блоков с однобитными входами). В результате приходим к вероятности 13-цикловой характеристики, равной

$$\left[\left(\frac{16}{64}\right)^4 \cdot \left(\frac{160}{64^2}\right)^2\right]^3 \cdot \left(\frac{16}{64}\right)^2 = 2^{-56}.$$

Теперь кратко остановимся на особенностях четырехцикловых характеристик остальных типов, поскольку приведенные выше рассуждения в значительной степени справедливы и для них. Характеристики вида 1.2 (рис. 2) минимального типа могут быть построены с использованием минимум пяти активных S-блоков, как это показано на рис. 3 (здесь при построении характеристики используются внутренние биты 6-битного входа S-блока). Нетрудно убедиться, что характеристики этого вида (с пятью активными S-блоками) и в неминимальном представлении используют нереализуемые однобитные переходы и переходы в ноль (они строятся с использованием циклического перехода). Нам не

удалось построить характеристик вида 1.2 неминимального типа, выходящих за ограничения разработчиков стандарта. Однако, как видно из представленных примеров и вида самой характеристики, представленной на рис. 2, для пар *S*-блоков, образующих циклы этой характеристики, выполняется ограничение У-2.

Отдельно следует отметить еще один тип характеристики 1.2 специфического вида, представленный на рис. 7.

Рис. 7

На этом же рисунке приведен пример построения подобной характеристики. Ее особенностью является переход одного из битов самого в себя. Можно убедиться, что такие характеристики и неминимального типа в каждом из циклов имеют *S*-блок с нулевым выходом. Эти итеративные характеристики и минимального (с шестью *S*-блоками) типа, и неминимального (с восемью *S*-блоками) типа подпадают под ограничение У-2 и поэтому опасности не представляют.

Что касается характеристики вида 1.3 (рис. 2), то из графа переходов для этой характеристики следует, что для ее осуществления должен одновременно выполняться целый набор циклических переходов. Анализ показывает, что для шифра DES этот набор переходов просто совместно неосуществим.

Таким образом, атаки ДК, использующие четырехцикловые итеративные характеристики, на алгоритм DES с таблицами, отобранными по требованиям разработчиков стандарта и дополнительному условию У-2, оказываются более сложными, чем прямой перебор ключей и, следовательно, становятся бессмысленными.

Остается заметить, что вероятность получения четырехцикловой характеристики с максимальными значениями вероятностей переходов сразу для всех активных *S*-блоков оказывается чрезвычайно малой. Поэтому с большой долей уверенности можно сказать, что *S*-блоки, отобранные только по критериям разработчиков стандарта, окажутся стойкими к ДК на основе четырехцикловых итеративных дифференциальных характеристик.

Список литературы: 1. *Лисицкая И.В., Головашич С.А., Олейников Р.В.* Построение таблиц подстановок для стандарта шифрования данных // Проблемы бионики. 1999. Вып 50. С. 185–194. 2. *Долгов В.И. Лисицкая И.В., Головашич С.А.* Принципы защиты алгоритма DES от атак дифференциального криптоанализа // Радиотехника. 2000. № 113. С. 148-157. 3. *Lysytska I.V., Koriak A.S., Golovashich S.A.* The selection criteria of random substitution tables for symmetric enciphering algorithms // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada. August 13-21. 1999. P. 204. 4. *Долгов В.И., Лисицкая И.В., Головашич С.А.* Обеспечение стойкости DES-подобных алгоритмов шифрования к атакам линейного криптоанализа при использовании подстановок случайного типа // Радиотехника. 2000. Вып 114. С. 39-46. 5. *K. Kim, S. Park, S. Lee.* Reconstruction of s^{2}DES S-boxes and their Immunity to Differential Cryptanalysis // Pros. of 1993 Korea-Japan Joint Workshop on Information Security and Cryptology (JW-ISC'93). Oct. 24-36. Seoul. 1993. 6. *L. R. Knudsen.* Iterative Characteristics of DES and s^{2}DES // Proc. of Crypto'92. UCSB. 1992. 7. *K. Kim, S. Lee and S Park.* Necessary Conditions to Strengthen DES S-boxes against Linear Cryptanalysis // Pros. of SCIS'94. Biwako. Japan. P. 1-11. Jan.27-29. 1994. 8. *K. Kim.* Construction of DES-like S-boxes Based on Boolean Function Satisfying the SAK // Pros. Of Asiacrypt'91. P. 59-72. Fujiyoshida. Japan. 1991. 9. *K. Kim, S. Lee, S. Park and D. Lee.* DES can be Immune to Linear Cryptanalysis // Workshop Record of SAC '94 (Selected Areas in Cryptography) May 5-6. Queen's Univ. Canada. 1994. 10. *K. Kim, S. Lee, S. Park.* How to Strengthen DES against Two Robust Attacks // Joint Workshop on Information Security and Cryptology Inuyata. Japan. January 24-25. 1995. 11. *Лисицкая И.В., Бондаренко А.С., Колыбельников А.И.* Обеспечение стойкости шифра DES к атакам линейного криптоанализа // Радиотехника. 2001. № 119. С. 45-55. 12. *E. Biham, A. Shamir.* Differential Cryptoanalysis of the full 16-round DES // Technical Report. Computer Science Department. Technion. Israiel. 1993. 13. *E. Biham, A. Shamir.* Differential Cryptanalysis of the Data Encryption Standard // Springer Verlag, Berlin. 1993. 14. *B. Schneier* Applied Cryptography. Second Edition: protocols, algorithms, and Source code in C // Published by John Wiley & SonS. Inc. New York: ChicheSter BriSbane Toronto Singapore. 1996. 758 p.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 05.04.2001